Ponemon Institute Report on Secure Flight Working Group

Prepared by Dr. Larry Ponemon, September 19, 2005

This report summarizes the work conducted by Ponemon Institute to help organize, prepare and finalize the Secure Flight Working Group's report for the Transportation Security Administration (TSA).

Appointed by the TSA, the Secure Flight Working Group (hereafter termed Working Group) is composed of nine individuals who have credentials in the privacy and security fields. The Secure Flight Working Group's sole objective was to provide advice and counsel to the TSA concerning privacy and data security considerations that might affect the Secure Flight program mission.

Engaged as a consultant to the TSA in mid-August 2005, our mission was defined as:

- First, to work with various members of the Working Group to obtain their unique insights and recommendations that might be incorporated in a confidential report.
- Second, to verify that the contributions made by the Working Group to the confidential report were accurately stated in accordance with various confidential source documents that reside on a secure extranet portal.
- Third, to determine if Secure Flight program activities were consistent with the program description contained in various confidential source documents that reside on a secure extranet portal.

The Working Group met three times between January and March 2005. Given the date of our engagement, we did not participate in any in-person meeting. Another consultant (Rand Corporation) assisted the Working Group by facilitating the three meetings. We relied on the written transcript and draft report in completing our project.

The Secure Flight Working Group Report

Individual members of the Working Group completed different sections (chapters) of the report. All Working Group members were given an opportunity to comment, edit and revise these sections. At different points in the document collection and editing process, we worked closely with individual authors to help them complete their contributions. At the outset, we made it clear that this was the Working Group's report. Our role was to organize their work into one coherent report. Following are nine chapters that were completed by Work Group members:

- Architecture
- Identity Matching
- Policy, Regulatory and Oversight Structure
- Watch Lists
- Test Phase – Commercial Data
- Passenger Screening
- Passenger Name Record
- Push versus Pull Model
- Data Retention Issues

Two sections were not completed by the Working Group. These are redress and security. In the case of security, the members responsible for this chapter said they did not have enough information.

Admittedly, the participation of Working Group members in the preparation of the report varied from significant to minimal. Those providing significant effort wrote one or more sections and made substantive editorial contributions during the report's final drafting.

After the first full draft was completed, we did a fact check on all references and citations provided in the report. Much of our fact check was based on documents residing on a secure extranet portal provided by the TSA to each member of the Working Group. Our fact checks proved that citations in the report are substantially accurate and complete.

Ponemon Institute's Validation of the Report

After completing the first full draft, I visited TSA's Secure Flight program offices to determine if the program documents reviewed by our team were consistent with actual Secure Flight program activities. While this review process did not include substantive auditing tests of the Secure Flight program, we did determine that the program description as contained in documents adequately reflects the program activities that exist today.

The *Report of the Secure Flight Working Group* (dated September 19, 2005) provides six questions reflecting the shared concerns of the nine person advisory group. As part of our accuracy checking procedures, we attempted to ascertain the validity of these questions. Much of what we learned is based on the review of Secure Flight program documentation, discussion with individual Working Group members, and in-person visit to the TSA's Secure Flight program office in Annapolis Junction in Maryland. Following are the Working Group questions with my perceptions and beliefs.

<u>What is the goal or goals of Secure Flight?</u>

The Working Group believes that "TSA apparently fails to understand the difference between program definition and program evolution. The definition of program goal may, of course, evolve, but at any given time, there must be a clear and exclusive definition of the program and its goals." It is my conclusion that the Working Group is correct in that we could not find a clear discussion about the goal or goals of the Secure Flight program in program documentation.

<u>What is the architecture of the Secure Flight System?</u>

According to the Working Group, "SFWG was provided limited information about the Secure Flight architecture, the analytic software that will be used or other software and hardware that will be used for data collection, processing, storage or deletion."

During my visit to the Secure Flight program office, I learned that decisions about the IT infrastructure (including vendor appointment), information security protections and use of commercial data sources were not made at the time the Working Group met in January and March 2005.

At present, the Secure Flight program's information security architecture is documented. Schematic illustrations and supporting documentation can now be viewed by members of the Working Group. With respect to the issue of PII from commercial data sources, these data elements will only be captured by the airlines and not from information brokers.

It is my belief the concerns raised by the Working Group about not having adequate information to evaluate the program's information security architecture is most likely to be true given that key documents did not exist at the time of the three Working Group meetings (and were not available on the extranet portal).

Secure Flight program office personnel also assured me that PII collected from different airline carriers is currently documented and mapped to specific applications. Despite these assurances, I believe that much more information about PII data flows is needed to gauge the privacy implications when using passenger's PII for screening purposes, especially if the Secure Flight program decides to enrich PII from commercial data sources at some point in the future.

Will Secure Flight be linked to other TSA applications?

To paraphrase the report, "The Working Group failed to obtain information about how the Secure Flight program will interact with other vetting programs operating on the same platform." At the time of the Working Group meetings in January and March 2005, much of the design for the identity vetting platform was not completed. Based on conversations with Secure Flight program personnel, it appears that the TSA now has a plan for coordinating different vetting applications that reside on one platform.

With respect to the larger issue of how Secure Flight will relate to other U.S. federal vetting and credentialing programs, it is unclear how identity vetting programs will be coordinated or managed to achieve maximum efficiency and effectiveness. We did not see any documents that described why the identity management process within Secure Flight was not linked or coordinated with other programs.

How will commercial data sources be used?

According to the Working Group report, "TSA has never clearly defined two threshold issues: what it means by 'commercial data'; and how it might use commercial data sources in the implementation of Secure Flight. Until these two fundamental issues are defined, and tests are conducted based on the defined uses, commercial data should not be implemented in Secure Flight."

As noted above, Secure Flight program leaders explained that commercial data sources were used in the early test phase. The use of commercial data in the pilot program was to improve the accuracy of the subject matching process.

Accordingly, the Secure Flight program will no longer use commercial data sources in its operations. Despite these assurances, I believe that the Working Groups concerns

about the inappropriate uses of commercial data are valid and must be considered if such data sources are ever used in the future.

What matching algorithms work best?

According to the Working Group report, "TSA never presented to the SFWG results of tests showing the effectiveness of algorithms used to match passenger names to a watch list." The Secure Flight program officials admitted that results of matching tests were not available at the time that the Working Group met in January and March. Statistical results of matching tests, including the impact of different methods on false positives, are now available for review.

On a separate, but related, concern raised by the Working Group about Watch List matching, the Secure Flight program officials did not provide any information about how they plan to manage synthetic identities (based on fake or breeder documents) as part of program efficacy. In short, we were unable to determine this from our evaluation of program documents or with discussions with program officials.

What is the oversight structure and policy for Secure Flight?

To paraphrase the Working Group report, "TSA has not produced a comprehensive policy document for Secure Flight program which defines oversight or governance responsibilities." Our review of documents did not reveal a comprehensive or clearly defined policy that defined oversight, governance and the accountability structure for the program. In short, I agree with the Working Group's assessment that Secure Flight program needs to have a uniquely defined policy that explains how it will be governed within or outside the TSA.

Conclusion

I believe that the Working Group attempted to ascertain the privacy and security risks inherent in the Secure Flight program. The issue of not having enough information to adequately judge key program attributes or features is very likely to be true. However, I believe it was due to the timing of the Working Group's evaluation of Secure Flight. The Working Group met prior to the TSA's completion of a conceptual design for Secure Flight. Therefore, they did not have access to information that might have addressed many of the questions raised in their report.

Finally, based on my meetings with key TSA personnel and review of the documents, TSA made reasonable efforts to communicate existing relevant information about Secure Flight with the Working Group members. In turn, the Working Group did make reasonable efforts to complete the report submitted on September 19, 2005.

Respectfully,

L.A. Ponemon

Dr. Larry Ponemon
Chairman, Ponemon Institute, LLC